NETWORKERS 2004

INTRODUCTION TO SNMP AND MIB

SESSION NMS-1N02

Objectives

- **This is an introduction on SNMP and MIB**
  - **For beginners**
  - **Will not delve into the technical details**
  - **SNMPv3: only an overview**
- **A preparation Networkers tutorials**
  - **A prerequisite for some Networkers tutorials**

Agenda

Cisco.com

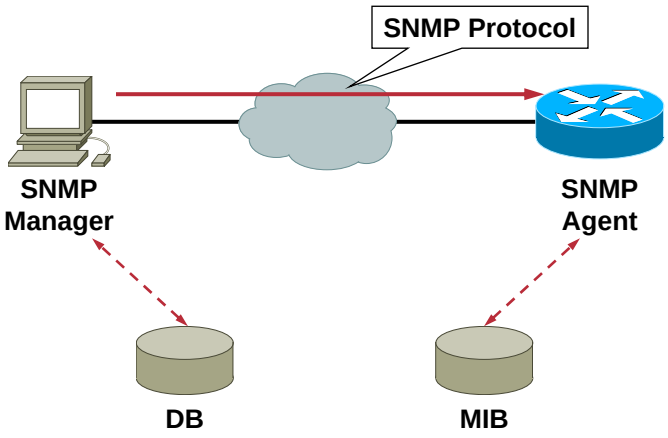
- Introduction
- SNMPv1—Everybody Should Know It
- SNMPv2c—The De Facto Standard
- All You Need to Know about MIBs
- Exercise
- SNMPv3—The Official Standard
- Notifications
- SNMP Summary

INTRODUCTION

The Basic Model

Cisco.com

Network Management Architecture



The Manager

Cisco.com

- The manager will try to provide solutions for FCAPS
  - Fault monitoring
  - Configuration control
  - Accounting monitoring
  - Performance monitoring
  - Security control

The Agent

Cisco.com

- **The agent is embedded on the device**
  - **The agent responds to requests for information and actions**
  - **The agent may send fault notification to the manager, i.e. a trap**
  - **The agent is exchanging managed information with the manager using the SNMP protocol**

The MIB

Cisco.com

- **The MIB is the collection of managed objects**
  - **The SMI—Structure of Management Information—defines the framework within which a MIB can be defined or constructed**
  - **The managed objects are arranged in a hierarchical tree**

THE PROTOCOL—SNMPV1 EVERYBODY SHOULD KNOW IT

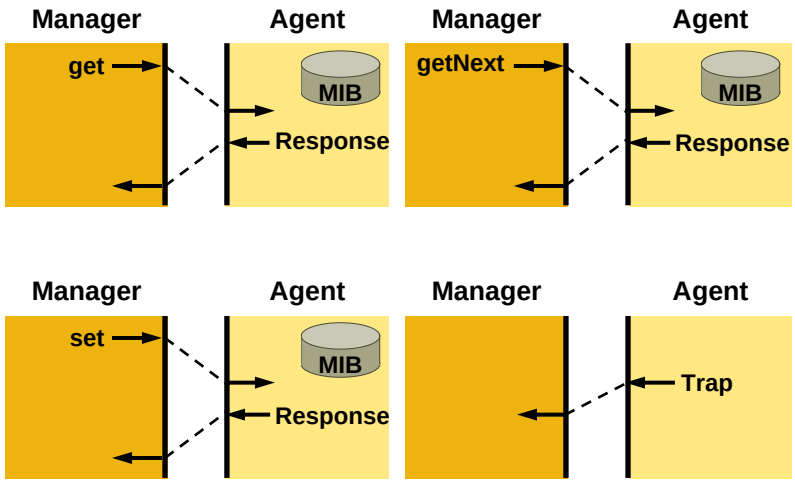
SNMPv1: The Protocol

Cisco.com

- **Everybody should know it**
  - **SNMP is the protocol between manager and agent**
  - **SNMPv1: UDP is specified as the transport protocol but no restriction per RFC**
  - **SNMPv1 is defined in RFC 1155, 1157, 1212**

SNMP Overview

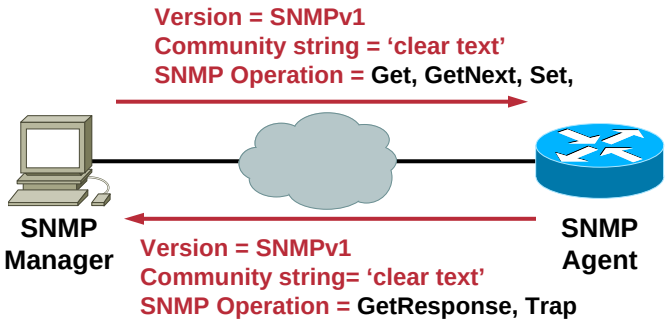
Cisco.com



SNMPv1: The Protocol

Cisco.com

- The SNMPv1 message



- No security in SNMPv1: the community strings are not encrypted

SNMPv1: The Community String

Cisco.com

- Simply defined as an OCTET STRING
  - Read community to GET MIB variables
  - Read-write community to GET and SET MIB variables
- Could contain any value: spaces, any character, or hex values that are not printable, etc.; but not always a good idea to use $, #, &, /,!
- So no limitations in terms on the length; the Cisco IOS limits the length to 128 bytes
- Don't use @ on the Catalyst; confusing with the community string indexing
  - Note: Same definition within SNMPv2c

SNMPv1: The Configuration

Cisco.com

```
Router(config)# snmp-server community public RO
Router(config)# snmp-server community private RW
Router(config)# snmp-server host 1.1.1.1 version
                1 public
Router(config)# snmp-server enable traps …
```

- Advice:
  - Do not use public and/or private as community strings
  - Do not use cisco…

SNMPv1: Access Control: The Access-List

Cisco.com

- An access-list associated with the community string

```
Router(config)# snmp-server community public RO 11
Router(config)# snmp-server community private RW 12
Router(config)# access-list 11 permit 172.17.246.225
Router(config)# access-list 11 permit 172.17.246.226
Router(config)# access-list 12 permit 172.17.246.225
```

- Limits which management stations can read or write to the device

SNMPv1: Access Control: The View

Cisco.com

- Limits which objects the management station can read or write
- How can we prevent the manager from polling the ARP and the routing tables?

```
Router(config)# snmp-server view myview iso included
Router(config)# snmp-server view myview atEntry excluded
Router(config)# snmp-server view myview ipRouteEntry excluded
Router(config)# snmp-server view myview internet.6.3.15 excluded
Router(config)# snmp-server view myview internet.6.3.16 excluded
Router(config)# snmp-server view myview internet.6.3.18 excluded
Router(config)# snmp-server community public view myview RO
```

SMIv1: Some SNMP Object Types

Cisco.com

- **INTEGER**
  - Length is 32 bits, can be negative
- **Gauge**
  - Length is 32 bits, an unsigned integer reflecting a current value
- **Counter**
  - Length is 32 bits, an unsigned counts something until it reaches its maximum value, then wraps
- **TimeTicks**
  - A measurement of time in hundredths of a second
- **OctetString**
  - 0 or more bytes of printable characters
- **IpAddress**

SNMPv1: How Gauges and Counters Work

Cisco.com

- **Gauge**
  - Like a speedometer
  - Used for rates like load (CPU, interface)
- **Counter**
  - Like an odometer
- **ATTENTION**
  - Counters do not necessarily start at zero, per standard
  - Counter can not be reset, per standard
  - Counters are not for direct human consumption
    - Require a DELTA function to compute rate

SNMPv1: Summary

Cisco.com

- No security in SNMPv1
- SNMPv1 uses Community Strings
- SNMPv1 includes MIB View concept
- SNMPv1 supports five operations
- SNMPv1 is supported on all the Cisco devices

THE PROTOCOL: SNMPV2C THE DE FACTO STANDARD

SNMPv2c: The Protocol

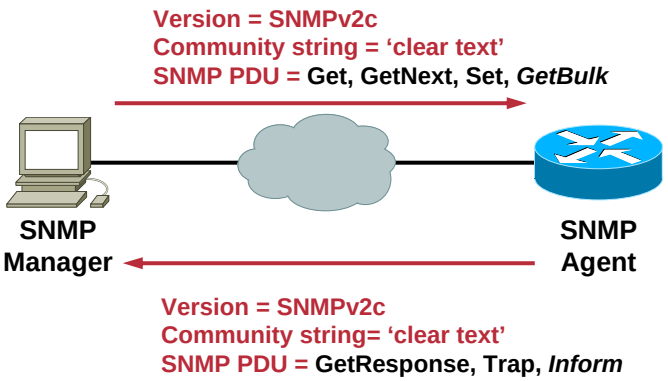
Cisco.com

- SNMPv2c is similar to SNMPv1, except
  - SNMPv2c supports the SNMPv2 additional operations:
    - getBulk
    - informRequest (a confirmed trap)
  - SNMPv2c supports new and renamed data types
    - Counter64, Counter32, etc.
  - SNMPv2c provides richer error handling
- SNMPv2c security is community-based
- SNMPv2 was abandoned
- SNMPv2c is defined in RFC 2578, 2579, 2580, 3416, 3417 and 3418

SNMPv2c: The Protocol

Cisco.com

- SNMPv2c security is coming from SNMPv1, based on communities



SNMPv2c: Counter Size

Cisco.com

- **RFC 2863 defines byte/packet counters widths**
  - **ifSpeed <= 20 Mbps**
    - **32-bit byte and packet counters**
  - **ifSpeed > 20 Mbps && < 650 Mbps**
    - **32-bit packet counters and 64-bit byte counters**
  - **ifSpeed >= 650 Mbps**
    - **64-bit byte and packet counters**
  - **Implementations may provide additional counters, i.e. 64-bit byte counters for 10M interfaces**

SNMPv2c Protocol Data Units (PDU)

Cisco.com

Get, GetNext, Set Request, Trap PDU, Inform

PDU Type	requestID	0	0	variableBindings

Response

PDU Type	requestID	errStatus	errIndex	variableBindings

(0) noError
(1) tooBig
(2) noSuchName
(3) badValue
(4) readOnly
(5) genError
etc…

Identifies the Variable Object in the Variable-Bindings List That Caused the Error, when the errStatus Field is Non-Zero

Note: GetBulk PDU Is a Slightly Different Format

SNMPv2c: Summary

Cisco.com

- SNMPv2c is based on SNMPv2
  - New operations (getBulk, informRequest)
  - New data types (Counter64, etc.)
  - Richer error handling
- SNMPv2c security: “no” security, as in SNMPv1
- Almost nothing changed from a configuration point of view, compared to version 1

ALL YOU NEED TO KNOW ABOUT MIBS

MIB Concepts

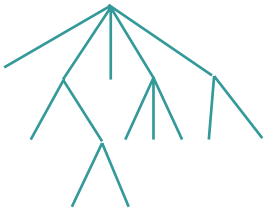
Cisco.com

- A MIB defines groups of attributes
  - Identifier -> how to refer to the attribute
  - Syntax -> basically its type
  - Access level -> who can see the attribute
- The SMI—Structure of Management Information—defines the framework within which a MIB can be defined or constructed
  - RFC 1155 specifies SMIv1
  - RFC 2578 specifies SMIv2
- Abstract Syntax Notation 1 (ASN.1) notation is used as language elements
- Basic Encoding Rule (BER) defines the elements coding

MIB Structure

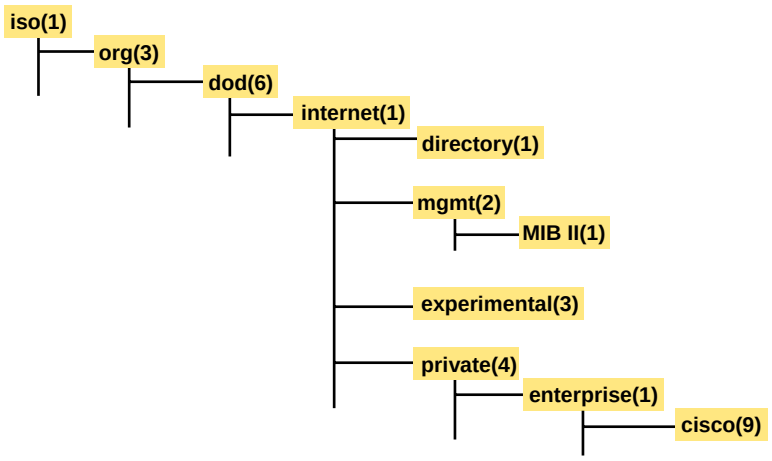
Cisco.com

- MIBs are hierarchically structured
  - Top levels controlled by IANA
  - Lower levels may be delegated
  - Each node given an integer identifier
  - Different MIBs may be combined into a tree structure
- Attributes are identified by specifying a "path" through the tree
  - Object Identifiers or OIDs
- Nodes may be given string valued names
  - Easier for "human" interaction
- A single device may support many MIBs
  - Device then appears to support the union of attributes from all the supported MIBs



The Object Identifier: OID

Cisco.com



The Object Identifier: OID

Cisco.com

- **Need a scheme that allows two vendors or products within a vendor to compare like items**
  - **Object Identifiers (OID) were chosen as the identification scheme**
  - **An OID is an ordered sequence of non-negative integers written left to right, containing at least two elements (0.0)**
  - **Bound to simple names in MIB Modules:**
    - **“ifInOctets” is 1.3.6.1.2.1.2.2.1.10**

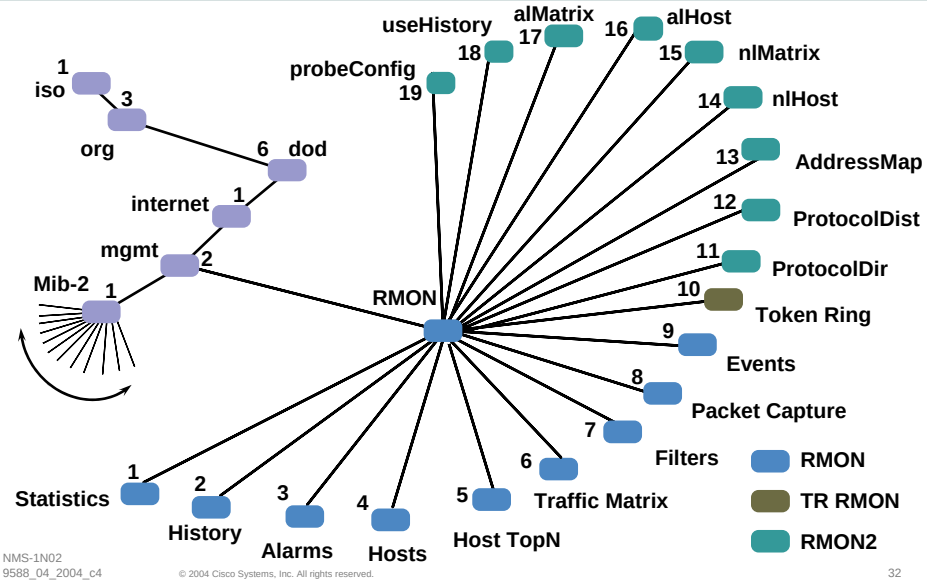
The Object Identifier: OID

Cisco.com

- **Once a MIB module is published, OIDs are bound for all time to the objects defined**
  - **Objects can not be deleted!**
  - **Can only be made obsolete**
  - **Even minor changes to an object are discouraged**

RMON MIB Object Identifiers

Cisco.com



How to Read a SMIv1 MIB Variable?

Cisco.com

```
sysDescr OBJECT-TYPE
              SYNTAX  DisplayString (SIZE (0..255))
              ACCESS  read-only
              STATUS  mandatory
              DESCRIPTION
                      "A textual description of the entity. This
    value should include the full name and version identification
    of the system's hardware type, software operating-system, and
    networking software.  It is mandatory that this only contain
    printable ASCII characters."
              ::= { system 1 }
```


How to Read a SMIv1 MIB Variable?

Cisco.com

```
object OBJECT-TYPE
        SYNTAX
        ACCESS
        STATUS
        DESCRIPTION
          “text”
        ::= { parent object-oid }
```

How to Read a SMIv1 MIB Variable?

Cisco.com

```
object OBJECT-TYPE
        SYNTAX
        ACCESS
        STATUS
        DESCRIPTION
          "text"
        ::= { parent object-oid }
```

OCTET STRING, OBJECT IDENTIFIER, INTEGER, IpAddress, Counter, Gauge, TimeTicks, etc…

How to Read a SMIv1 MIB Variable?

Cisco.com

```
object OBJECT-TYPE
        SYNTAX
        ACCESS
        STATUS
        DESCRIPTION
          "text"
        ::= { parent object-oid }
```

OCTET STRING, OBJECT IDENTIFIER, INTEGER, IpAddress, Counter, Gauge, TimeTicks, etc…

read-only
read-write
write-only
not-accessible

How to Read a SMIv1 MIB Variable?

Cisco.com

```
object OBJECT-TYPE
        SYNTAX
        ACCESS
        STATUS
        DESCRIPTION
          "text"
        ::= { parent object-oid }
```

OCTET STRING, OBJECT IDENTIFIER, INTEGER, IpAddress, Counter, Gauge, TimeTicks, etc…

read-only
read-write
write-only
not-accessible

mandatory
optional
obsolete

SMIv1—Some SNMP Object Types

Cisco.com

- **INTEGER**
  - Length is 32 bits, can be negative
- **Gauge**
  - Length is 32 bits, an unsigned integer reflecting a current value
- **Counter**
  - Length is 32 bits, an unsigned counts something until it reaches its maximum value, then wraps
- **TimeTicks**
  - A measurement of time in hundredths of a second
- **OctetString**
  - 0 or more bytes of printable characters
- **IpAddress**

How to Read a SMIv2 MIB Variable?

Cisco.com

```
sysDescr OBJECT-TYPE
                SYNTAX      DisplayString (SIZE (0..255))
                MAX-ACCESS  read-only
                STATUS      current
                DESCRIPTION
            "A textual description of the entity. This value
    should include the full name and version identification of the
    system's hardware type, software operating-system, and
    networking software."
                ::= { system 1 }
```


How to Read a SMIv2 MIB Variable?

Cisco.com

```
object OBJECT-TYPE
        SYNTAX
        MAX-ACCESS
        STATUS
        DESCRIPTION
          “text”
          ::= { parent object-oid }
```

How to Read a SMIv2 MIB Variable?

Cisco.com

```
object OBJECT-TYPE
        SYNTAX
        MAX-ACCESS
        STATUS
        DESCRIPTION
          "text"
          ::= { parent object-oid }
```

OCTET STRING,
OBJECT IDENTIFIER,
INTEGER, IpAddress,
Counter32,
Counter64,
Unsigned32,
Gauge32,
TimeTicks, etc…

How to Read a SMIv2 MIB Variable?

Cisco.com

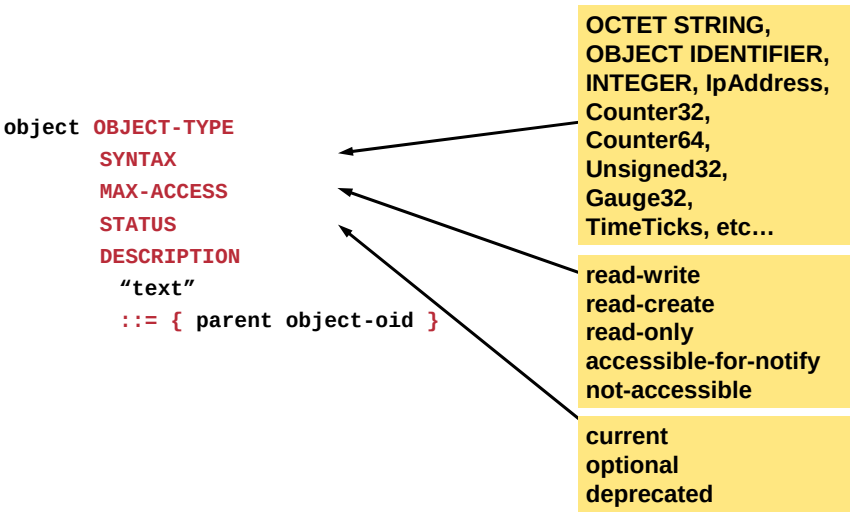
```
object OBJECT-TYPE
        SYNTAX
        MAX-ACCESS
        STATUS
        DESCRIPTION
          "text"
          ::= { parent object-oid }
```

OCTET STRING,
OBJECT IDENTIFIER,
INTEGER, IpAddress,
Counter32,
Counter64,
Unsigned32,
Gauge32,
TimeTicks, etc…

read-write
read-create
read-only
accessible-for-notify
not-accessible

How to Read a SMIv2 MIB Variable?

Cisco.com



SNMPv2 and v2c—New Data Types

Cisco.com

- **Integer32**
  - Length is 32 bits, can be negative
- **UInteger32**
  - Still 32 bits, but non-signed
- **Gauge32**
  - An integer reflecting a current value
- **Counter32 and Counter64**
  - Only counters come in 64 bits size
  - Counts something until it reaches its maximum value, then wraps

SNMP Indexing

Cisco.com

- A Device consist of many SNMP objects

  EG Power supply, CPU, interfaces

- Object instances are identified by unique indexes

  Example: devices have multiple interfaces, each will have a unique index

1: ifDescr.1 (octet string) Ethernet0/0
2: ifDescr.2 (octet string) Serial0/0
3: ifDescr.3 (octet string) Serial0/1
4: ifDescr.4 (octet string) Loopback0

Device has 4 interfaces, indexed 1–4

All interface references will use these index numbers

How to Read a SMIv2 MIB Table?

Cisco.com

```
ifTable OBJECT-TYPE
            SYNTAX  SEQUENCE OF IfEntry
            MAX-ACCESS  not-accessible
            STATUS  current
            DESCRIPTION
            "A list of interface entries. The number of entries is given
  by the value of ifNumber."
            ::= { interfaces 2 }

 ifEntry OBJECT-TYPE
            SYNTAX  IfEntry
            MAX-ACCESS  not-accessible
            STATUS  current
            DESCRIPTION
            "An interface entry containing objects at the subnetwork
  layer and below for a particular interface."
            INDEX   { ifIndex }
            ::= { ifTable 1 }
```

How to Read a SMIv2 MIB Table?

Cisco.com

```
IfEntry ::=
            SEQUENCE {
                 ifIndex
                      INTEGER,
                 ifDescr
                      DisplayString,
                 ifType
                      IANAifType
                …
                 }

ifIndex OBJECT-TYPE
            SYNTAX  InterfaceIndex
            MAX-ACCESS  read-only
            STATUS  current
               DESCRIPTION
                    "A unique value for each interface.  Its value ranges
  between 1 and the value of ifNumber.  The value for each interface must
  remain constant at least from one re-initialization of the entity's
  network management system to the next re-initialization."
            ::= { ifEntry 1 }
```


The Table Index in SMI

Cisco.com

- No limitation in number of indexes
- No limitation in the variable type

  Integer, IpAddress, Octetstring
- No persistence by default

```
router(conf) snmp-server ifindex persist
router(conf-if) snmp-server ifindex persist
```

How to Test a MIB?

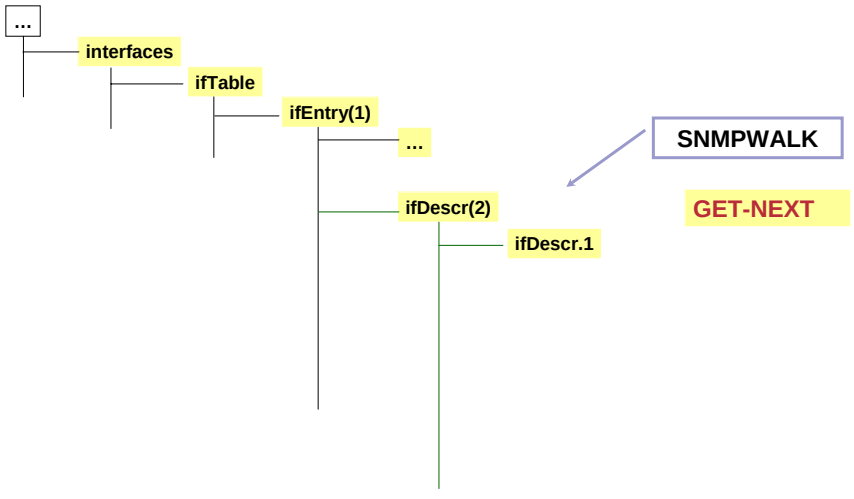
Cisco.com

```
NMS# snmpwalk <router> <community_string> ifTable.1.2
  interfaces.ifTable.ifEntry.ifDescr.1 : ethernet0/0
  interfaces.ifTable.ifEntry.ifDescr.2 : serial0/0
  interfaces.ifTable.ifEntry.ifDescr.3 : serial0/1
  interfaces.ifTable.ifEntry.ifDescr.4 : loopback0

NMS# snmpwalk <router> <community_string> ipRouteDest
  ip.ipRouteTable.ipRouteEntry.ipRouteDest.5.5.5.5 :
  IpAddress:   5.5.5.5
  ip.ipRouteTable.ipRouteEntry.ipRouteDest.1.1.1.0 :
  IpAddress: 1.1.1.0
```

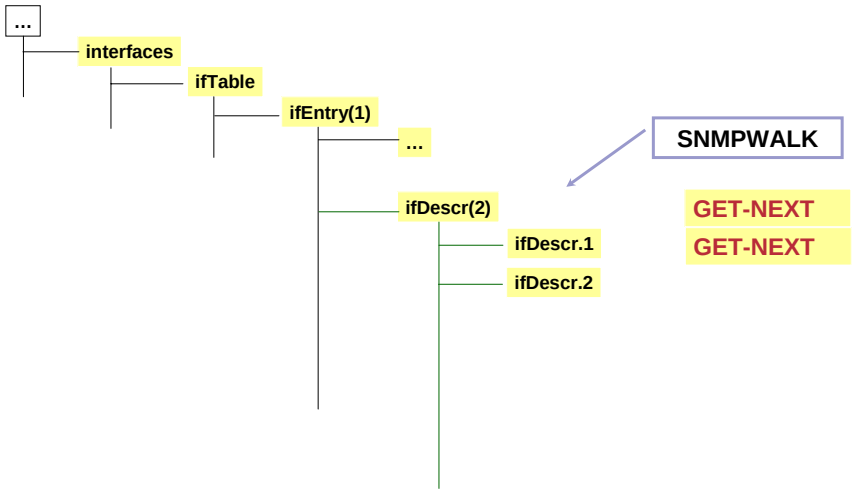

Snmpwalk with several GET-NEXT (V1)

Cisco.com



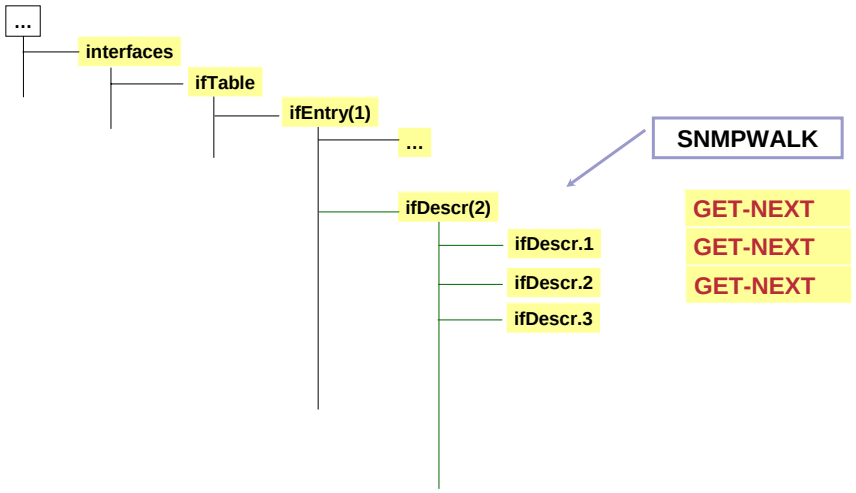
Snmpwalk with several GET-NEXT (V1)

Cisco.com



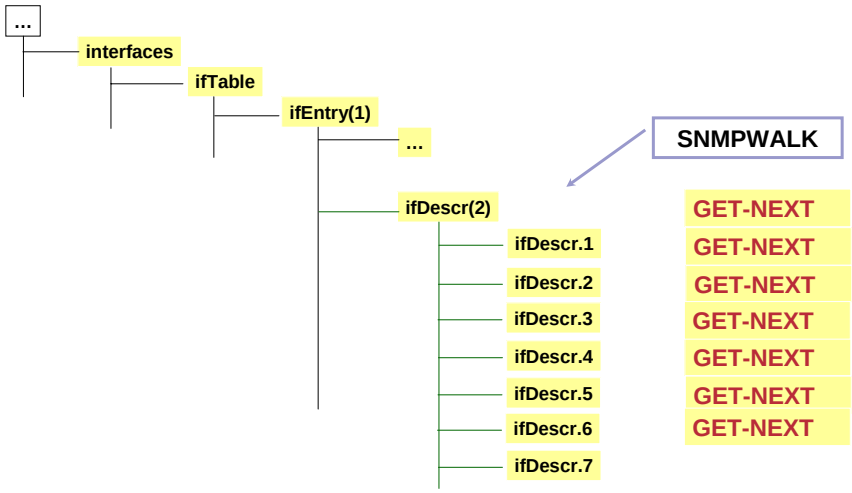
Snmpwalk with several GET-NEXT (V1)

Cisco.com



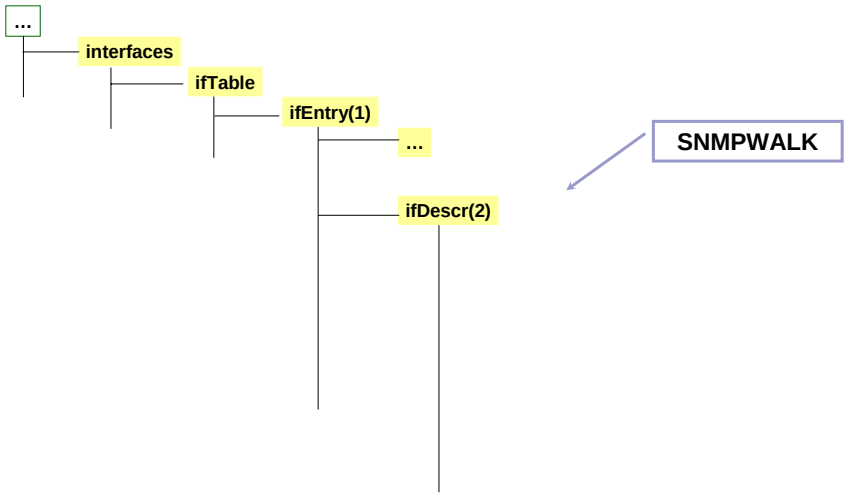
Snmpwalk with several GET-NEXT (V1)

Cisco.com



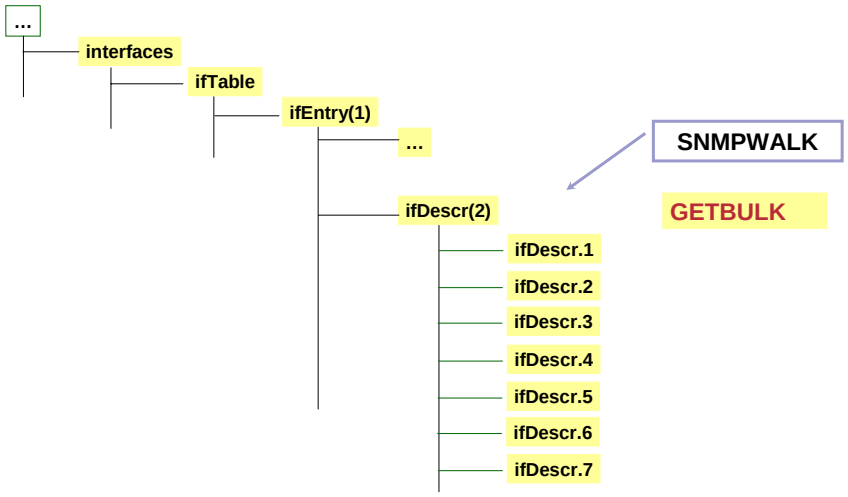
Snmpwalk with GETBULK (V2c)

Cisco.com



Snmpwalk with GETBULK (V2c)

Cisco.com



Polling an Object

Cisco.com

- SNMP GET request
  - Same idea for SET request
- Need to specify
  - IP address of agent
  - Community string to gain access
  - OID of attribute

Polling an Object

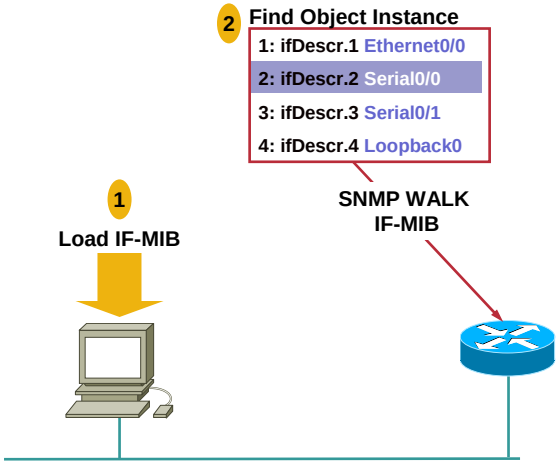
Cisco.com

- SNMP GET request
  - Same idea for SET request
- Need to specify
  - IP address of agent
  - Community string to gain access
  - OID of attribute

Polling an Object

Cisco.com

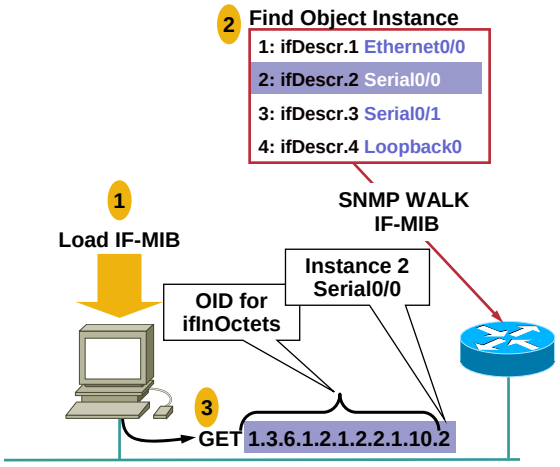
- SNMP GET request
  - Same idea for SET request
- Need to specify
  - IP address of agent
  - Community string to gain access
  - OID of attribute



Polling an Object

Cisco.com

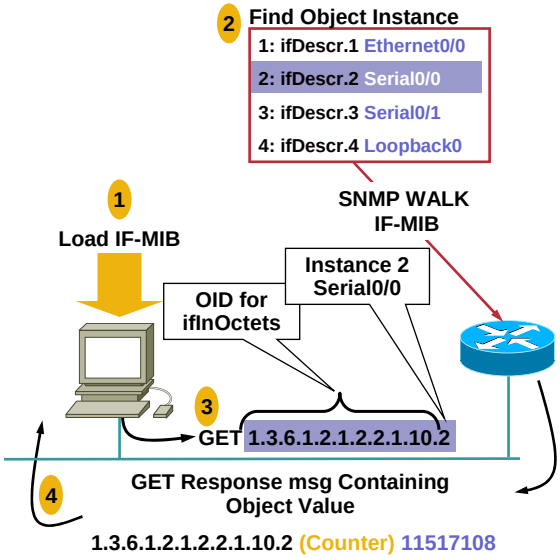
- SNMP GET request
  - Same idea for SET request
- Need to specify
  - IP address of agent
  - Community string to gain access
  - OID of attribute



Polling an Object

Cisco.com

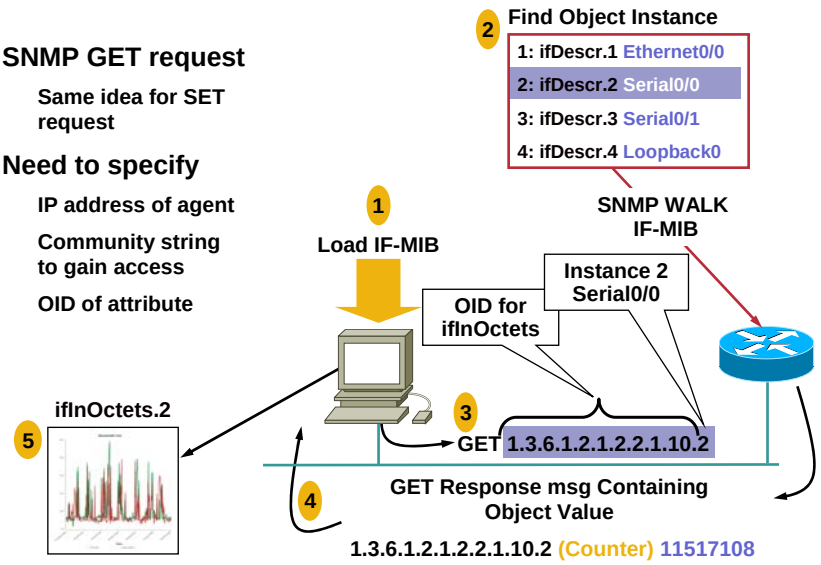
- SNMP GET request
  - Same idea for SET request
- Need to specify
  - IP address of agent
  - Community string to gain access
  - OID of attribute



Polling an Object

Cisco.com

- SNMP GET request
  - Same idea for SET request
- Need to specify
  - IP address of agent
  - Community string to gain access
  - OID of attribute



Polling an Object

Cisco.com

- Identify what objects need to be polled
  - Examples, Interface bytes, Interface packets, CPU utilization
- Load MIBs into the management station
  - So management station knows how to poll the device
  - To provide human form
- Identify the object instance number
  - Example, for a device with multiple interfaces, each interface will have a unique index number
- Identify the object type
  - Counters require delta calculations to be meaningful
  - Gauges provide an absolute value

How to Find Out about a MIB Variable?

Cisco.com

- **MIB Locator in CCO**

  http://www.cisco.com/go/mibs

- **FTP site:**

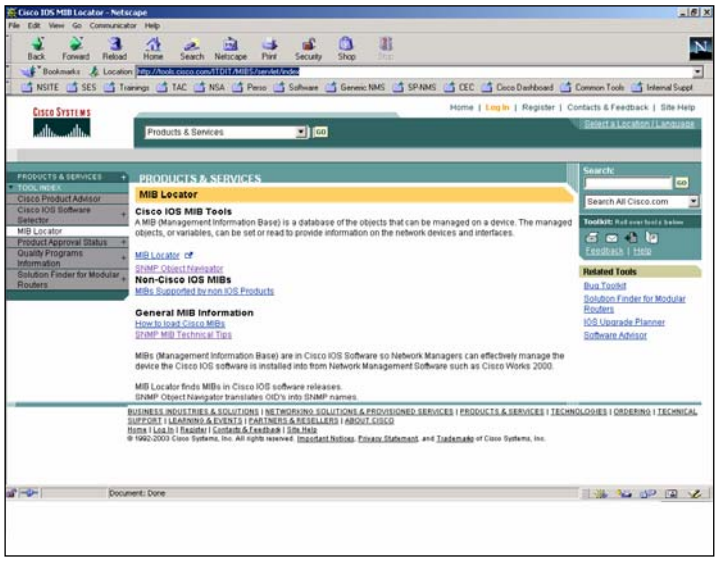
  ftp://ftp.cisco.com/pub/mibs

- **External site:**

  http://jaguar.ir.miami.edu/%7Emarcus/snmptrans.html

http://www.cisco.com/go/mibs

Cisco.com



MIB Locator in CCO

Cisco.com

- **MIB Locator**
  - Which MIBs are supported for my platform?
  - Which MIBs are supported for my Cisco IOS® train?
  - Which MIBs are supported for my specific image?
  - Where (platform, Cisco IOS, image) is this MIB supported?
- **SNMP Object Navigator**
  - Search for MIB variable
  - What is the MIB variable for a specific OID?
  - To which MIB does it belong to?
  - What is the definition?
  - Hierarchy in the tree?

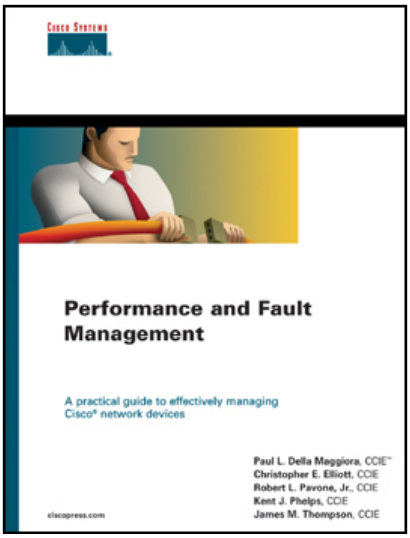
Important MIBs

Cisco.com

- **MIB II -> RFC1213**
- **Interfaces Group MIB -> RFC 2863**
- **RMON1 MIB -> RFC 2819**
- **RMON2 MIB -> RFC 2021**
- **Etc.**

Which MIB Variables to Monitor?

Cisco.com

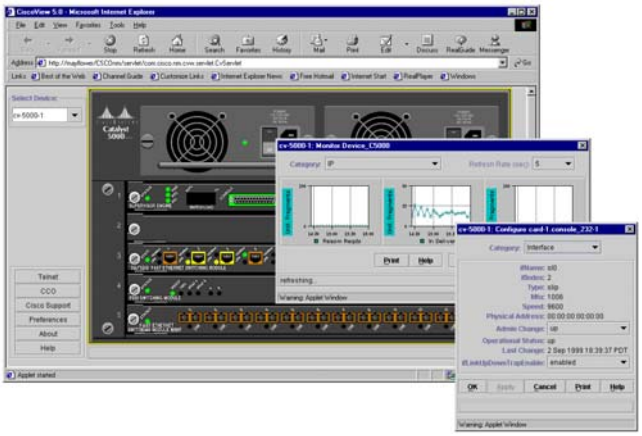


EXERCISES

Exercise 1

Cisco.com

- Goal: find via SNMP the status of an interface
- How does CiscoView determine the interface color?



Exercise 1: Response

Cisco.com

- SNMP Object Navigator
- Look for interface or ifTable or status
- Find ifAdminStatus and ifOperStatus
- snmpwalk on the ifAdminStatus and ifOperStatus
- Look at the index (ifIndex)
- Look at ifDescr
- snmpwalk on the ifDescr
- Correlate with the ifIndex
- Try to use snmpset…

- Note: download any snmp utility

  For example, http://www.net-snmp.org/tutorial/commands/

Exercise 1: Response

Cisco.com

```
NMS# snmpwalk <router> public ifAdminStatus
       interfaces.ifTable.ifEntry.ifAdminStatus.1 = up(1)
       interfaces.ifTable.ifEntry.ifAdminStatus.2 = up(1)
       interfaces.ifTable.ifEntry.ifAdminStatus.3 = down(2)
       …

NMS# snmpwalk <router> public ifOperStatus
       interfaces.ifTable.ifEntry.ifOperStatus.1 = up(1)
       interfaces.ifTable.ifEntry.ifOperStatus.2 = up(1)
       interfaces.ifTable.ifEntry.ifOperStatus.3 = down(2)
       …

NMS# snmpwalk <router> public ifDescr
       interfaces.ifTable.ifEntry.ifDescr.1 = Serial0/0
       interfaces.ifTable.ifEntry.ifDescr.2 = Serial0/1
       interfaces.ifTable.ifEntry.ifDescr.3 = Serial0/2
       …
```


Exercise 1: Response: A Different Way!

Cisco.com

```
NMS# snmpwalk <router> public ifDescr
       interfaces.ifTable.ifEntry.ifDescr.1 = Serial0/0
       interfaces.ifTable.ifEntry.ifDescr.2 = Serial0/1
       interfaces.ifTable.ifEntry.ifDescr.3 = Serial0/2
       …

NMS# snmpget <router> public ifAdminStatus.3
       interfaces.ifTable.ifEntry.ifAdminStatus.3 = down(2)

NMS# snmpget <router> public ifOperStatus.3
       interfaces.ifTable.ifEntry.ifOperStatus.3 = down(2)
```

Exercise 1: Response: A Different Way!

Cisco.com

```
Router# sh snmp mib ifmib ifindex
     Serial0/0: Ifindex = 1
     Serial0/1: Ifindex = 4
     Serial0/2: Ifindex = 3
     …

NMS# snmpget <router> public ifAdminStatus.3
     interfaces.ifTable.ifEntry.ifAdminStatus.3 = down(2)

NMS# snmpget <router> public ifOperStatus.3
     interfaces.ifTable.ifEntry.ifOperStatus.3 = down(2)
```


Exercise 2

Cisco.com

- Goal: find via SNMP the equivalent of:

```
router# show tcp brief
TCB          Local Address      Foreign Address          (state)
813BF810     cointreau.23       dhcp-peg3-cl3114.32881   ESTAB
813B41A0     20.0.0.1.179       20.0.0.2.22138           ESTAB
```

Exercise 2: Response

Cisco.com

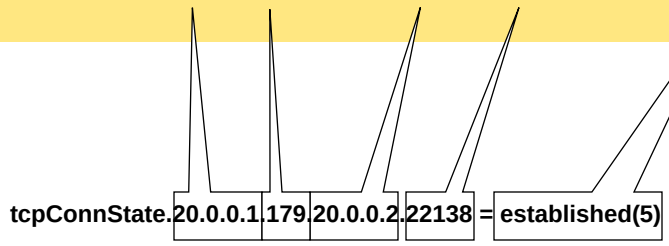
- **tcpConnTable, with 4 indexes: tcpConnLocalAddress, tcpConnLocalPort, tcpConnRemAddress, tcpConnRemPort**

```
NMS# snmpwalk cointreau public tcpConnTable
tcpConnState.10.48.71.7.23.144.254.5.46.32881 = established(5)
tcpConnState.20.0.0.1.179.20.0.0.2.22138 = established(5)
tcpConnLocalAddress.10.48.71.7.23.144.254.5.46.32881 = IpAddress: 10.48.71.7
tcpConnLocalAddress.20.0.0.1.179.20.0.0.2.22138 = IpAddress: 20.0.0.1
tcpConnLocalPort.10.48.71.7.23.144.254.5.46.32881 = 23
tcpConnLocalPort.20.0.0.1.179.20.0.0.2.22138 = 179
tcpConnRemAddress.10.48.71.7.23.144.254.5.46.32881 = IpAddress: 144.254.5.46
tcpConnRemAddress.20.0.0.1.179.20.0.0.2.22138 = IpAddress: 20.0.0.2
tcpConnRemPort.10.48.71.7.23.144.254.5.46.32881 = 32881
tcpConnRemPort.20.0.0.1.179.20.0.0.2.22138 = 22138
```


Exercise 2: Response

Cisco.com

```
router# show tcp brief
TCB          Local Address      Foreign Address          (state)
813BF810     cointreau.23       dhcp-peg3-cl3114.32881   ESTAB
813B41A0     20.0.0.1.179       20.0.0.2.22138           ESTAB
```



THE PROTOCOL—SNMPv3 THE OFFICIAL STANDARD

What's New in SNMPv3?

Cisco.com

SNMPv3 Defines Two Security-Related Capabilities:

- The User-Based Security Model (USM) provides
  - Authentication (user/password)
  - Privacy (encryption)
  - Note: operates at the message level
- The View-Based Access Control Model (VACM)
  - Determines whether a given principal (user) is allowed access to particular MIB objects to perform particular functions
  - Note: Operates at the PDU Level

SNMPv3 Framework

Cisco.com

- RFC 3410: Introduction and Applicability Statements for Internet-Standard Management Framework
- RFC 3411: An Architecture for Describing SNMP Management Frameworks
- RFC 3412: Message Processing and Dispatching for SNMP
- RFC 3413: SNMPv3 Applications
- RFC 3414: User-Based Security Model (USM) for version 3 of SNMPv3
- RFC 3415: View-Based Access Control Model (VACM) for SNMP
- RFC 3584: Coexistence between version 1, 2, and 3 of SNMP

SNMPv3 Framework

Cisco.com

- The existing SNMPv1 and SNMPv2c PDUs must be used within the new architecture
- An implementation referred to as SNMPv3 consists of the security and architecture features defined in RFC 3410 through 3415 plus the PDU format and functionality defined in the SNMPv2c documents
- Hence no new SNMPv3 PDUs defined
- SNMPv1, SNMPv2c, SNMPv3 are sharing the same basic structure and components:

  Manager, agent, protocol, management information
- Hence no SMI version 3 defined

SNMPv3: Security Subsystem

Cisco.com

- The only security model is the User-Based Security Model for SNMPv3: RFC 3514
- Security Model performs authentication and privacy function
- Authentication is related to user/password
- Privacy is related to disclosure: encryption

  Note: Privacy requires an Cisco IOS image with encryption

SNMPv3: Security Subsystem (Cont.)

Cisco.com

AuthNoPriv	NoAuthNoPriv
AuthPriv	~~NoAuthPriv~~

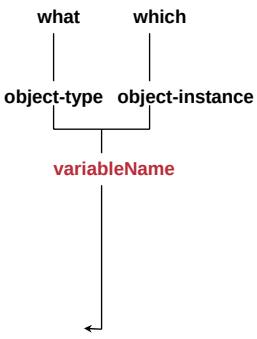
- Not possible because the privacy key is linked to a user
- We must have authentication to have privacy

SNMPv3
View-Based Access Control Model Logic

Cisco.com

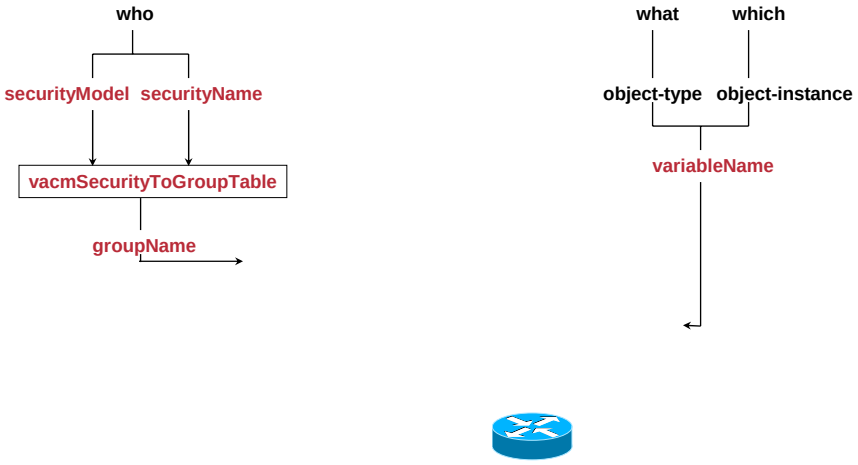
SNMPv3
View-Based Access Control Model Logic

Cisco.com



SNMPv3
View-Based Access Control Model Logic

Cisco.com

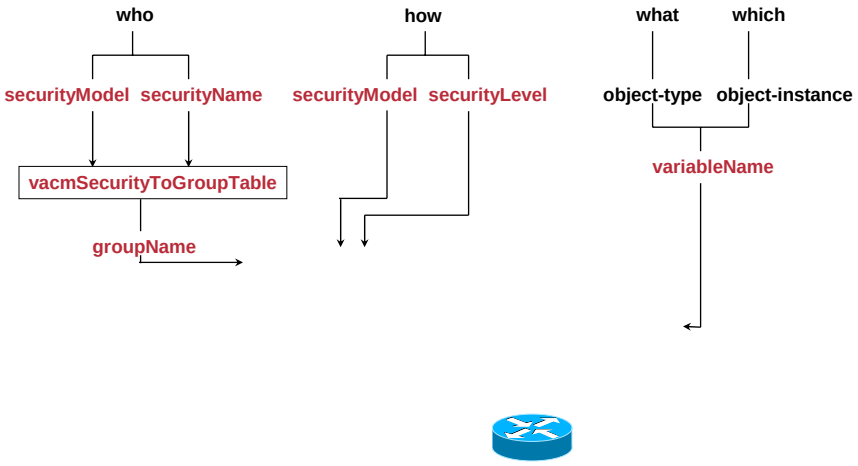


NMS-1N02
9588_04_2004_c4

85

SNMPv3
View-Based Access Control Model Logic

Cisco.com

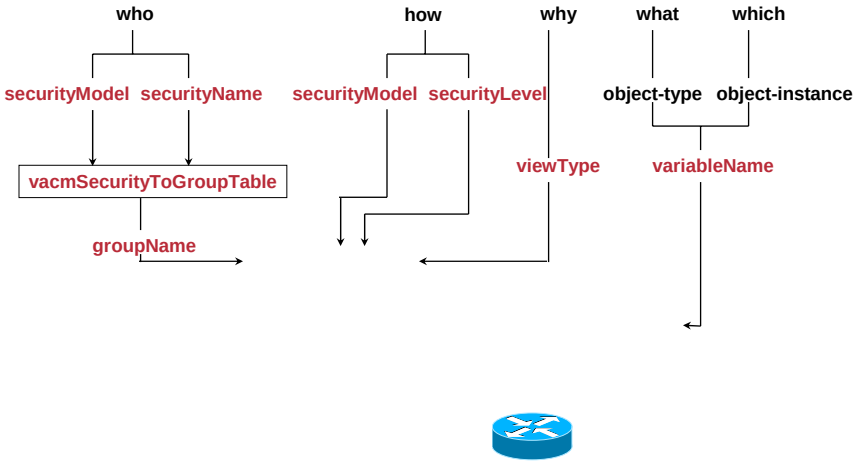


NMS-1N02
9588_04_2004_c4

86

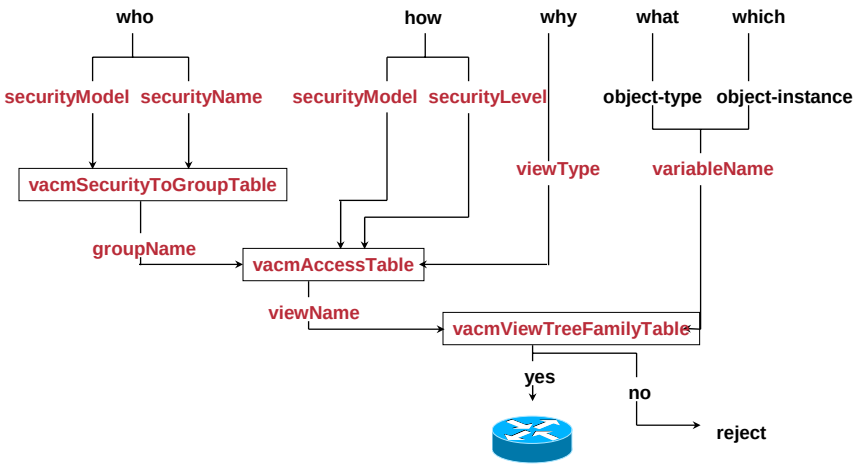
SNMPv3
View-Based Access Control Model Logic

Cisco.com



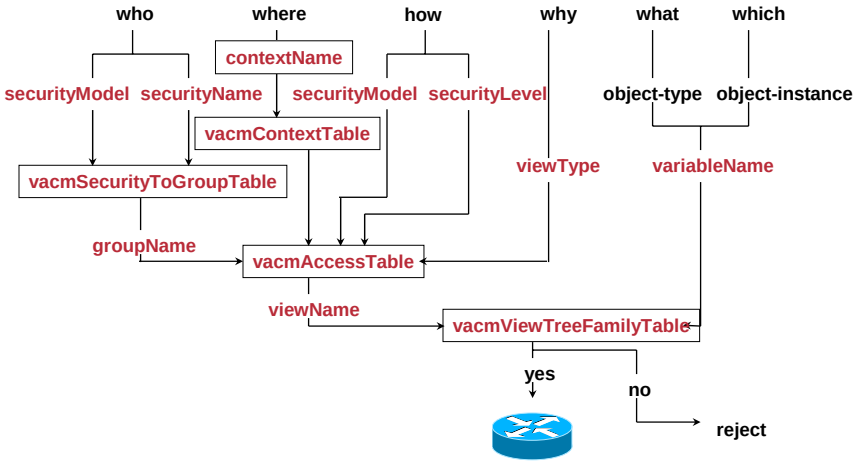
SNMPv3
View-Based Access Control Model Logic

Cisco.com



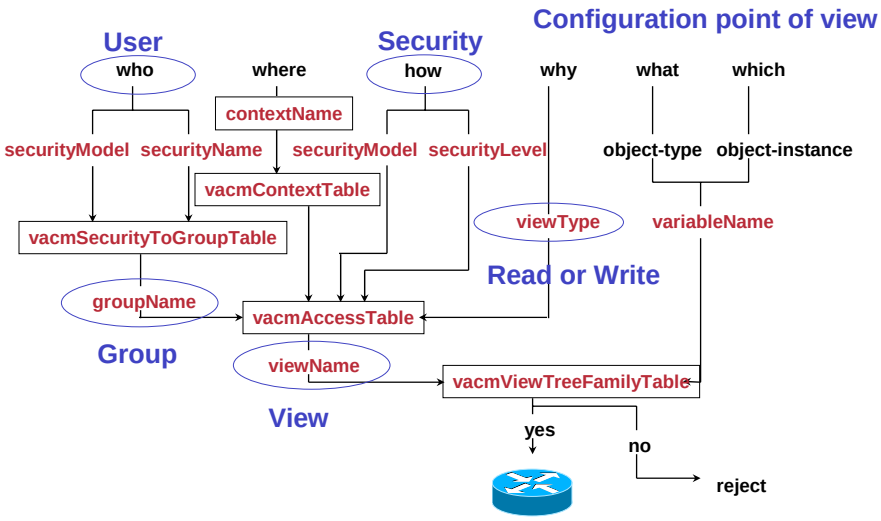
SNMPv3
View-Based Access Control Model Logic

Cisco.com



SNMPv3
View-Based Access Control Model Logic

Cisco.com



SNMPv3 Configuration Example

Cisco.com

```
Router(config)# snmp-server engineID local
                123456789012345678901234
Router(config)# snmp-server user joe joegroup v3 auth
                md5 joepassword
Router(config)# snmp-server group joegroup v3 auth
```

- **Joe belongs to Joegroup:**
  - **securityLevel is authNoPriv**
  - **No MIB View**

SNMPv3 Configuration Example

Cisco.com

```
Router(config)# snmp-server user bill billgroup v3
Router(config)# snmp-server group billgroup v3 noauth
                read billview
Router(config)# snmp-server view billview internet included
Router(config)# snmp-server view billview cisco excluded
Router(config)# snmp-server view myview internet.6.3.15 excluded
Router(config)# snmp-server view myview internet.6.3.16 excluded
Router(config)# snmp-server view myview internet.6.3.18 excluded
Router(config)# snmp-server community public ro
```

- **Bill belongs to Billgroup**
  - **securityLevel is noAuthNoPriv**
  - **Has read access on MIB view 'billview' which includes MIB-II and excludes private cisco MIB**

SNMPv3: Attention with the View

Cisco.com

```
Router(config)# snmp-server view myview iso included
Router(config)# snmp-server view myview atEntry excluded
Router(config)# snmp-server view myview ipRouteEntry excluded
Router(config)# snmp-server view myview internet.6.3.15 excluded
Router(config)# snmp-server view myview internet.6.3.16 excluded
Router(config)# snmp-server view myview internet.6.3.18 excluded
Router(config)# snmp-server community public view myview RO
```

- The default Views restrict the access to the USM, VACM and COMMUNITY MIBS
- Pay attention not to enable a security holes when playing with views in SNMPv3!

NOTIFICATIONS

How to Enable SNMP Notification?

Cisco.com

- On a Cisco Router:

```
Router (config)# snmp-server enable traps
<trap_type>
Router (config)# snmp-server host <NMS host>
version <v1/v2c/v3 [auth | noauth | priv]>
<trap_community> <trap_type>
```

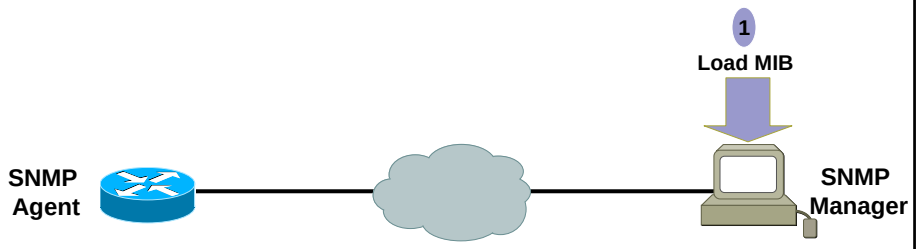
- Trap Type: isdn, snmp, tty, envmon, entity, config, bgp, frame-relay, etc.
- The notification is sent to UDP port 162

SNMP Trap Notification

Cisco.com

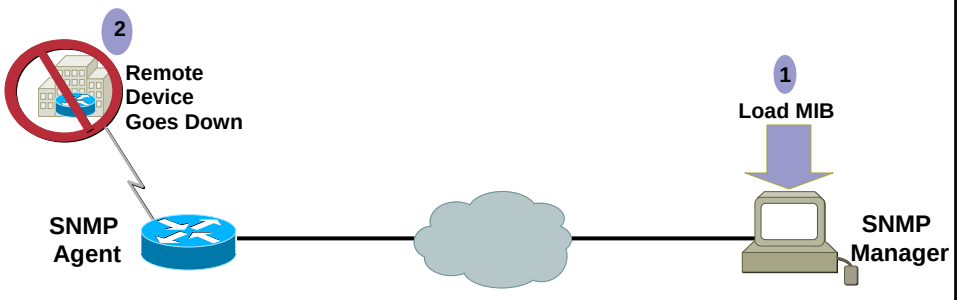
SNMP Trap Notification

Cisco.com

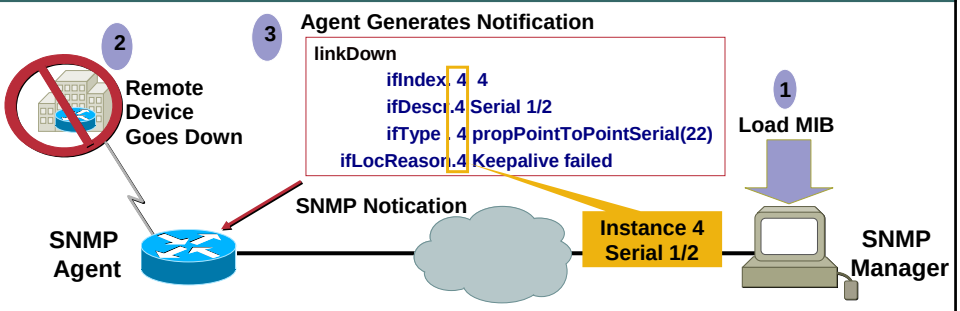


SNMP Trap Notification

Cisco.com



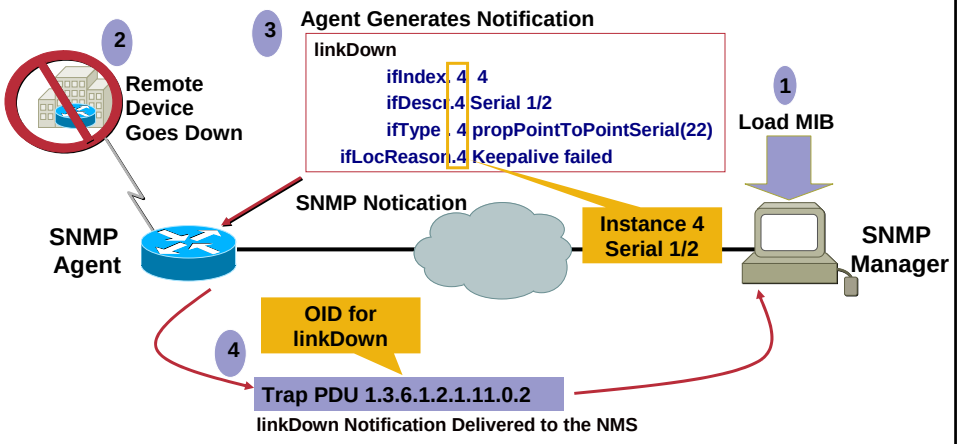
SNMP Trap Notification



SNMP trap notification contains:

Varbinds: ifIndex, ifDescr, ifType, ifLocReason

SNMP Trap Notification



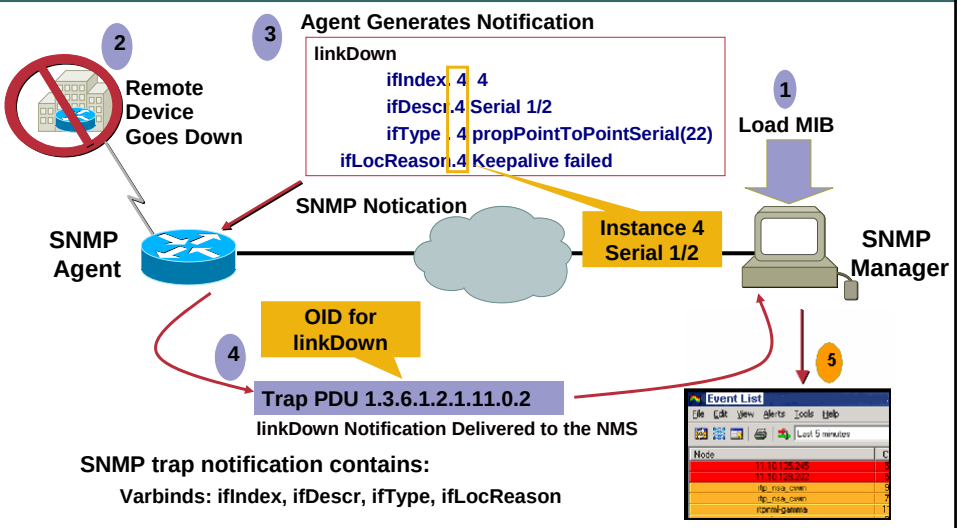
SNMP trap notification contains:

Varbinds: ifIndex, ifDescr, ifType, ifLocReason

OID: linkDown Notification

SNMP Trap Notification

Cisco.com



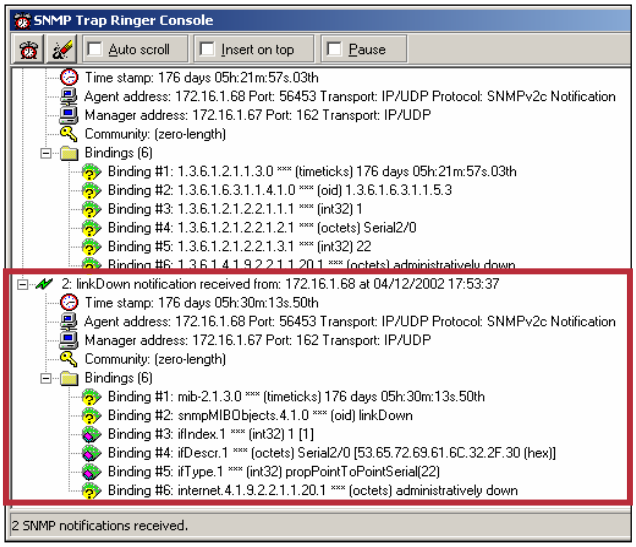
SNMP trap notification contains:

Varbinds: ifIndex, ifDescr, ifType, ifLocReason

OID: linkDown Notification

What if the MIB Is Not Loaded in the NMS?

Cisco.com



The Operator Gets Strings of OIDs

With IF-MIB Installed, Descriptions Have Replaced the String of Numbers

SNMP SUMMARY

SNMP Versions

Cisco.com

	Level	Auth	Encryption	What Happens
SNMPv1	noAuthNoPriv	Community String		Uses a Community String Match for Authentication
SNMPv2c	noAuthNoPriv	Community String		Uses a Community String Match for Authentication
SNMPv3	noAuthNoPriv	Username (*)		Uses a Username Match for Authentication
SNMPv3	authNoPriv	MD5 or SHA		Provides Authentication Based on HMAC-MD5 or HMAC-SHA Algorithms
SNMPv3	authPriv	MD5 or SHA	DES	Adds DES 56-bit Encryption in Addition to Authentication Based on DES-56

(*) Like a Community String

SNMP Basics: Cisco IOS Versions

Cisco.com

SNMPv1	Since 10.3
SNMPv2	10.3, 11.0, 11.1, 11.2
SNMPv2c	11.3, 12.0, 12.0(3)T, 12.0(6)S, 12.1, 12.2, 12.3
SNMPv3	12.0(3)T, 12.0(6)S, 12.1, 12.2, 12.3

Conclusion

Cisco.com

- Good background information about SNMP and MIBs
- Prepared to attend any Networkers NMS tutorials
- Thank you

Other Network Management Sessions

Cisco.com

- NMS-1N01—Introduction to Network Management—Networkers Online
- NMS-1N02—Introduction to SNMP and MIBs—Networkers Online
- NMS-1N03—Accurate Time Synchronization—Networkers Online
- NMS-1N04—Introduction to Service Assurance Agent—Networkers Online
- NMS-1N41—Introduction to Performance Management—Networkers Online
- NMS-1011—Principles of Fault Management
- NMS-1101—Understanding DNS and DHCP
- NMS-2001—Network Troubleshooting Tools and Techniques
- NMS-2021—Large Scale Deployments of CiscoWorks

Other Network Management Sessions (Cont.)

Cisco.com

- NMS-2031—Traffic Accounting Scenarios
- NMS-2032—NetFlow for Accounting, Analysis and Attack
- NMS-2042—Performance Measurement with Cisco IOS
- NMS-2051—Securely Managing Your Network
- NMS-2102—Deploying and Troubleshooting NAT
- NMS-2101—DNS Deployment and Operation
- NMS-3011—Getting the Right Fault Events from Network Elements
- NMS-4012—MPLS Embedded Management Tools
- NMS-4043—Advanced Service Assurance Agent
- NMS-2T00—Network Management Best Practices—Techtorial